IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	:	
	:	
v.	:	1:21CR418-1
	:	
RASHAWN ERIC MCEACHERN	:	
	:	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

NOW COMES the United States of America, by and through Sandra J. Hairston, United States Attorney for the Middle District of North Carolina, and hereby files this response in opposition to the defendant's motion to suppress, and states the following in support thereof:

I. OVERVIEW

Rashawn Eric McEachern ("McEachern") is charged in a two-count Indictment, alleging receipt of child pornography (Count One), in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (Count Two). *See* Docket Entry No. (DE #1).

This case involves Freenet. Freenet is a peer-to-peer file-sharing network whose design is intended to permit users to remain anonymous while distributing files to and from each other. However, despite its goal of keeping

hidden the identity of its users, the nature of Freenet's design allows the use of a statistical technique, to determine with a high degree of accuracy, the Internet Protocol ("IP") address of a Freenet user that requests (or downloads) illicit child pornography files. This technique was first described in a paper published in May of 2017 in the *Proceedings of the IEEE International Workshop on Privacy Engineering* by several academic computer scientists at the University of Massachusetts-Amherst and Rochester Institute of Technology ("the Authors"). Levine et al, *Statistical Detection of Downloaders in Freenet* (2017), Exh. C, DE # 22-3, hereafter, "2017 Article."[1] The Authors published a second peer-reviewed paper in 2020 regarding the same technique. Levine et al, *A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet* (2020), hereto as Exh. C, hereafter, "2020 Article." The details of the technique, and its particular application in this case, are summarized in greater detail below.

In 2021, the aforementioned technique was applied to determine that a

[1] The undersigned expects to call Dr. Brian N. Levine and retired North Carolina State Bureau of Investigation Special Agent Rodney White as expert witnesses. The Government has previously disclosed the curriculum vitaes (CV) of both witnesses to counsel for the defendant. Dr. Levine's CV and Special Agent White's CV are attached hereto as Exhibit A and Exhibit B, respectively. To the extent descriptions of the Freenet network, the statistical technique and method used by law enforcement or facts related to White's investigation are not cited, the Government expects the witnesses to testify to those matters with more details and fewer simplifications.

Freenet user operating a computer assigned to IP address 71.71.101.240 had attempted to download nine known child pornography files in September and October of 2021. Law enforcement determined, via returns from an administrative subpoena issued for subscriber information of the IP address, that the subscriber was Rashawn McEachern at 3051 Bluebird Lane, Apt. 206, Mebane, North Carolina ("McEachern's residence").

On October 20, 2021, law enforcement used the foregoing technique and information in its affidavit for probable cause to obtain a state search warrant for McEachern's residence and devices therein, issued by North Carolina Superior Court Judge William A. Wood ("the Warrant"). *See* Exh. A to Def. Motion to Suppress, DE #22-1.[2] Law enforcement seized multiple devices from McEachern's residence. One of the items seized during the search was a G Skill Desktop Tower. McEachern admitted that the desktop computer that he built was his.

During a forensic examination of the G Skill Desktop and the associated Western Digital Hard Drive, law enforcement located 10,415 image files and 2,458 video files depicting child pornography with creation dates from June 12,

[2] Counsel for defendant attached as Exhibit A, the Affidavit for Probable Cause and not the full search warrant. For consistency, the government will refer to that Exhibit when referencing the Warrant.

2020 through October 17, 2021. The nine child pornography files of interest in the investigation were located in a Freenet downloads folder. The instant indictment followed.

On March 21, 2022, McEachern filed the instant motion to suppress evidence obtained as a result of the execution of the Warrant at his residence, contending that it lacked probable cause. *See* DE #22. McEachern contends that the method used by law enforcement to identify McEachern's IP address as the most likely used to request child pornography is arbitrary and inaccurate. (DE #22 at 2-3).

The Warrant was amply supported by probable cause to believe that someone using the IP address at McEachern's residence had requested child pornography files through Freenet and, accordingly, that evidence of child pornography crimes would be located there. Even if the warrant was deficient, law enforcement reasonably relied upon its issuance by a neutral and detached judicial official and the *Leon* good faith exception applies to bar suppression of evidence. Accordingly, the motion to suppress evidence should be denied.

II. STATEMENT OF FACTS

A. Background on Peer-to-Peer Networks and Freenet

Peer-to-Peer ("P2P") file sharing networks allow their users to share and receive electronic files, including images, and videos, with a network of other

users. To exchange files, users' computers communicate directly with each other, rather than through central servers. *See Metro–Goldwyn–Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919–20 (2005). Freenet is an example of one such network.

According to Freenet's website, Freenet's focus is to provide a place on the Internet for free speech and anonymity. *See* https://freenetproject.org/pages/about.html (last accessed 4/7/2022). Freenet is often used to advertise and distribute images and videos depicting child pornography.[3]

In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. *See id*. The underlying computer code (i.e., "source code") for Freenet is open and publicly available to anyone with the qualifications to read and understand it. That means that Freenet is an "open source" software.[4]

Freenet uses a system of distributed storage and retrieval of files. Computers on the Freenet network ("nodes") must contribute to the network bandwidth and a portion of their hard drive for storage, so that files uploaded

[3] In the 2017 Article and the 2020 Article (collectively "the Scientific Articles"), the Authors explain that at least 30% of Freenet traffic was for child pornography related files. *See* Exh.C at 1-3; *see also* DE #22-3 at 2.

[4] Since the source code for the software is open, users may modify Freenet to a certain extent.

(or "inserted") to Freenet can be distributed and stored across the network. *See id*. Files can be uploaded or downloaded from the Freenet network. Importantly, nodes on Freenet only connect directly with a certain selected group of other nodes (its "peers"). The IP addresses of a node's peers are visible to it, but a node cannot see the IP address of nodes other than its peers.

Unlike some P2P networks, computers using Freenet do not host specific files from their own collection. Instead, when a user uploads a file into Freenet, the software breaks the file into encrypted pieces called "content blocks" or "blocks," each of which is identified on the network through a unique hash value. Exh. C at 3. The bigger the size of the file, the more blocks will be created. The computer of the uploader (node) then distributes the blocks to its peers. *Id*. A peer may store the block on the hard drive it made available to Freenet or may send it along to its peers to store. *Id*. Whether a block is immediately stored or sent on to one of its own peers is a function of the Freenet software, not an individual user's decision. Because the pieces are encrypted, a Freenet network user is unable to access the content of pieces that are stored as blocks on his or her hard drive.

When the node distributes the content blocks, it also inserts a separately encrypted manifest block. *Id*. The manifest block contains the list of blocks for the file and the hash value. *See id*. When the upload of the file is successful,

the Freenet software returns to the uploader a decryption key and a "manifest key"—a series of letters, numbers and special characters—that is necessary to download the file. *See id*. at 2.

That user can then share the manifest key with other Freenet users, so that other users can also download the entire file. The manifest key is often shared on public forums. For much of the child exploitation material available on Freenet, the manifest keys are made publicly available via Freenet-based websites called "Freesites" and message boards such as those found on Frost, an application within Freenet that provides discussion groups organized by topic.

When a user wants to retrieve a particular file from Freenet, the user enters the manifest key associated with the file in the downloads section of Freenet. The requesting computer ("node" or "requester") first obtains the manifest block associated with the file, and then submits requests to its peers for the content blocks comprising the file, as described in the manifest. The requester then attempts to collect all of the stored encrypted pieces (blocks) of that file from its peers.

A node making a request for a content block selects a peer essentially at random from which to request the block. Consequently, given the number of block requests, the total number requests are divided up roughly equally

among the user's peers. If the peer possesses the requested block, it passes the block back to the requesting node. If the peer does not possess the requested block, it passes the request to one of its own peers, again resulting in a roughly equal division of relayed requests among the peer's own peers. This process continues until the requested block is found and passed back to the requesting node, or until the request expires. Thus, there are two types of requesters, the original requester—the one attempting to download (a downloader) the file; and the relaying requester—the one that is merely relaying the original request (a relayer).

To prevent unfulfilled requests from circulating endlessly through the network, Freenet assigns each request a lifespan in the form of a numerical value known as "hops to live" (HTL). By default, a request is initially assigned an HTL of 18, and (with the exception described below) is decremented each time it is relayed from one node to another. When a request's HTL reaches 0, the request is not further relayed and, instead, a "not-found" error is returned to the requesting node. If no adjustments were made to this system, it would be obvious to a Freenet node (including, for example, one operated by law enforcement), whenever it received a request from a peer with HTL 18, that the peer submitting the request was the original requester of the file of which the requested block formed a part, as opposed to merely passively relaying a

request originally made by another (non-peer) node. The identity of users requesting particular files (in the form of their IP addresses) would thus be revealed to their peers.

Freenet attempts to counteract this by decrementing HTL 18 requests only with 50% probability. This coin flip is conducted by the node as to each of its peers (not as to each request), and the decision is permanent as to that peer. Thus, with respect to roughly 50% of its requests,[5] a node submitting an original request will immediately decrement the request and transmit a request with HTL 17, and with respect to the other roughly 50%, will decline to decrement and send requests with HTL 18. Moreover, nodes receiving requests with HTL 18 and relaying them to other nodes will decrement those requests only if original requests sent to that particular peer would also have been decremented. Consequently, when a node receives a request with HTL 17 or 18, the peer submitting the request may or may not have been the original requester of the blocks requested. This feature of Freenet's design is intended to conceal the identity of the original requester.

Thus, Freenet attempts to provide anonymity to its users by hiding the identity of users who upload and download files on Freenet. Requests by

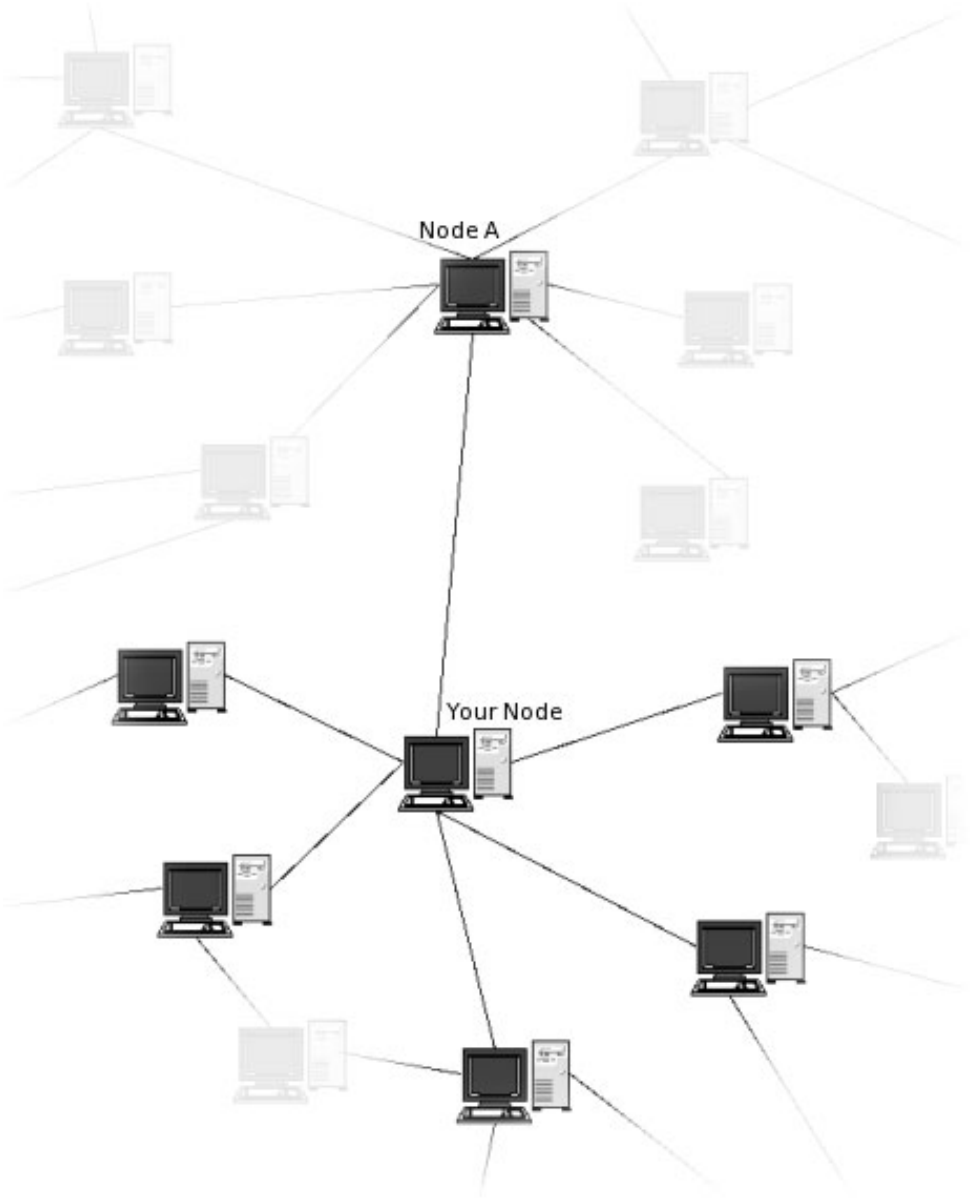
[5] As noted above, because requests are made to a node's peers essentially at randomly, they are submitted in roughly equal numbers to each of its peers.

Freenet users are routed through multiple other users' computers to make it more difficult to determine which user is the original requester of blocks of a particular file. Freenet warns its users, however, that when using the "opennet" operational mode of Freenet (as pertinent to this case) there is limited anonymity. *See* https://freenetproject.org/pages/help.html. [6] For example, Freenet explains that statistically, it can be shown that a particular user is more likely to have been the user who requested a file (rather than a user who merely forwarded a request for a file) based on an analysis of information such as the proportion of the pieces of a file requested by a user, the locations of nearby peers, and other characteristics about the request. *Id*.

As previously noted, the IP addresses of users' "peer" computers are visible to a particular user. For example, if a Freenet user is connected to six peers, the user can see all 6 of his peers' IP addresses on his screen. Freenet provides Figure 1, "Visible Freenet connections" to help explain the visibility of users:

---

[6] There are two operational modes on Freenet: "opennet" mode and "darknet" mode. *See id*. ("…'darknet' mode [is] where your Freenet node (software on your computer) only connects to the Freenet nodes run by [a user's] friends, i.e. people [the user] knows"). Opennet mode on the other hand "connect[s] automatically to whoever the network assigns, rather than connection to only their friends." *Id*. The method used in this investigation is uses only opennet. Exh. C at 3.



https://freenetproject.org/pages/documentation.html.

Thus, Freenet does not specifically attempt to mask a computer's IP address, which is commonly used to identify the location of a particular computer user. As such, Freenet provides its users with many warnings about the potential of being identified when using the opennet operational

mode of Freenet.

B. Statistical Technique

In the Scientific Articles, the Authors describe a rigorously-derived statistical technique that effectively distinguishes between block requests from a downloader and those from a relayer. The mathematical details of the technique are most comprehensively described in the Scientific Articles themselves. *See* DE # 22-3; Exh. C. In simple terms, however, the technique basically proceeds from intuitive observation that nodes submitting original requests for large files will submit requests for a larger number of blocks, spread randomly among its peers; conversely, those merely relaying the original requests will submit for only a fraction of those blocks, having distributed the larger number of requests received from an original requester randomly among its own peers. The mathematical technique establishes a statistical technique that—given certain inputs, such as the number of download requests submitted to a node by a peer, the number of nodes directly connected to that peer, and the total number of requests that an original downloader would submit in order to obtain a file—distinguishes between a downloader and a relayer.

The Authors of the 2017 Article tested the statistical technique both on a simulated network constructed similarly to the Freenet network, and on

actual Freenet data recorded by passive Freenet nodes operated by the Authors. *See* DE # 22-3. The Authors found the statistical technique was highly reliable. *See id.* at 2, 8.

In the 2020 Article, which was peer-reviewed, the Authors sought to clarify aspects of and further evaluate its statistical technique. *See* Exh. C. The 2020 Article does not reflect any changes to the method or software used by law enforcement to identify IP addresses of likely downloaders of child pornography files. Recognizing that law enforcement "investigators require a method that is both effective and *forensically sound*," the Authors adopted the *Daubert* standard[7] as their definition of "forensically soundness." *Id.* at 2. They sought a method that "is based on a testable hypothesis, has a known error rate, follows existing standards, and uses generally accepted methods." *Id.*

Through use of a spectrum of evaluations, the Authors again found the statistical technique was highly reliable. *See* Exh. C. Of particular interest was the evaluation of the method through real-world deployment of nodes in the Freenet network. [8] *See id.* at 6-8. The testing occurred from October of 2017 until April of 2020. *Id.* at 6. Without the knowledge of law enforcement,

[7] *Daubert v. Merrell Dowell Pharmaceutical*, 509 U.S. 579 (1993).
[8] Referred to as "in situ testing."

the Authors deployed nodes to Freenet that only relayed requests for blocks and waited to see what happened in the real world use of the algorithm. *Id.* They found the false positive rate to be less than 1%. *Id.* Ultimately, the Scientific Articles revealed the statistical technique is forensically sound.

C. The Affidavit and Application of the Statistical Technique to the Defendant

In the affidavit for the Warrant of McEachern's residence, Special Agent Rodney White introduced himself as an investigator of computer crimes and internet crimes against children assigned to the Computer Crimes Unit of the North Carolina Bureau of Investigation ("NCSBI"). DE# 22-1 at 2. White listed his qualifications, including specialized training in computer forensics Computer Network Investigations, and specialized training in undercover P2P internet investigations—which included Freenet, Gnutella, ARES, eMule, and BitTorrent networks. *Id.*

Based on White's training and experience, as well as information received from other law enforcement officers and/or agents, White described at length the background into Freenet, including what happens when a user uploads a file to the Network and what happens when a user attempts to download a file using Freenet. *Id.* at 3-6. Included was an example of how Freenet operates when a user attempts to download a file, which included

visual figure 1 and figure 2. *Id*. In a discussion involving these figures, he indicates that the "design can help law enforcement distinguish between a [Freenet] user that is the original requestor [sic], and one that is merely forwarding the request of another user." *Id*. at 6. The affidavit also includes information regarding Freenet's knowledge that it can be "statistically shown" that a particular user can be shown to be the likely original requester "based on factors including the proportion of the pieces of the file requested and the number of nearby peers." *Id*.

The affidavit also provides information related to child pornography on Freenet and law enforcement's investigation of child pornography on Freenet. *Id*. at 6-7. In the latter, it references the use of a modified version of the Freenet software to log information related to requests for blocks and the collection of child pornography keys. *Id*. at 7. White indicated that by reviewing the data from the abovementioned log, "it is possible to determine whether it is significantly more probable than not that the peer is the original requester of a file of interest" by applying a "mathematical formula…to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another." *Id*.

A Freenet node operated by law enforcement officers observed requests

for blocks comprising portions of nine separate child pornography files of interest submitted on separate occasions in September and October of 2021 by a peer using the IP address 71.71.101.240. DE # 22-1 at 7-11. As the affidavit to the Warrant made clear, "With respect to each file—considering the number or requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had—the number of requests for file pieces is significantly more than one would expect to see if the user of IP address were merely routing the request to another user." *Id.* at 8.

Each of the observed requests sought portions of known child pornography files, each of which was known to be available on Freenet (because a file with the same unique hash value had been downloaded by the affiant), as explicitly described in the affidavit. *Id.* at 8-10. This included the specified numbers for the average number of the requester's peers, the number of pieces requested from the law enforcement computer, and the total number of pieces needed to assemble the file. *See id.*

White also observed the child pornography-related activity of the node assigned to the IP address 71.71.101.240. *See id.* at 8-11. The affidavit provided that "[w]hile it is not an absolute certainty the user was the original request, with respect to each file, considering the number of requested blocks the total number of blocks required to assemble the file, and the number of

peers the user had, the number of requests for blocks of the file is significantly more than one would expect to see if the suer of IP address were merely routing the request of another user." *Id* at 8.

After determining this, law enforcement sought subscriber information from Charter Communications, the relevant internet service provider. *Id*. at 10. Charter Communications provided records that the subscriber of the for IP address 71.71.101.240 was McEachern, residing at McEachern's residence. *Id*. Based upon an affidavit containing a general description of Freenet, its relationship with child pornography, a summary of the statistical technique at issue, and its application to the defendant, the issuing judicial officer found that probable cause was established, and the Warrant was issued for McEachern's residence.

D. The Search

On October 20, 2021, investigators, including White, executed the search authorized by the Warrant. McEachern was present at the residence. Investigators seized several devices, including a G Skill Desktop McEachern said he built. During a forensic review of the Desktop, and hard drives within, White located 10,415 image files and 2,458 video files depicting minors, including prepubescent minors, engaged in sexually explicit conduct. The files were located in a Freenet downloads folder and a Frost Downloads folder,

including all nine of the child pornography files that were subject to the statistical technique that supported probable cause for the Warrant.

III. LEGAL ISSUES

A. . Probable Cause Supported the Issuance of the Search Warrant Based on the Reliable Methodology and Identification of McEachern's IP Address

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Subject to a few exceptions, this guarantee requires law enforcement to obtain a valid warrant prior to conducting a search. *See United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018). Such warrants must be "issued by a neutral magistrate and supported by probable cause." *United States v. Montieth*, 662 F.3d 660, 664 (4th Cir. 2011); *see* U.S. Const. amend. IV.

In determining probable cause, judges "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 339 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)); *see also Ornelas v. United States*, 517 U.S. 690, 696 (1996). ("probable cause to search [] exist[s] where the known facts and circumstances are sufficient to warrant a man of

reasonable prudence in the belief that contraband or evidence of a crime will be found").

The probable cause inquiry is "not a high bar." *Bosyk*, 933 F.3d at 339 (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). To that end, the Supreme Court has expressly recognized that affidavits in support of search warrants should not be subject to "'[t]echnical requirements of elaborate specificity," and that a judge has the "authority ... to draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant.'" *United States v. Bynum*, 293 F.3d 192, 197 (4th Cir. 2002) (quoting and citing *Gates*, 462 U.S. at 235, 240).

Where a judge issues a challenged warrant, reviewing courts do not "assess probable cause de novo." *Id*. Instead, courts "limit [their] inquiry to whether there was a substantial basis for determining the existence of probable cause." *Monteith*, 662 F.3d at 664 (internal quotation and citation omitted). In so doing, courts "accord great deference to the magistrate's assessment of the facts presented … [but] may not go beyond the information actually presented to the magistrate during the warrant application process." *Lyles*, 910 F.3d at 791.

Application of the principles described above to the instant case reveals that the affidavit described strong evidence to believe the user of IP address

71.71.101.240 was the original requester on his devices. As noted above, the algorithm is mathematically sound and was described in great detail by the Authors, who are established academic computer scientists. The statistical technique has been evaluated in Freenet itself with the in situ testing, in simulations of network with a Freenet-like structure, and using actual data collected from Freenet. The evaluations show the technique to be extremely reliable, with a false positive rate of less than 1%. Indeed, the results of the search warrant support that algorithm used is reliable: the nine child pornography files detailed in the search warrant were located on McEachern's device at his residence.

To ensure forensic soundness, the Authors used the *Daubert* standards their own. The 2020 Article was peer-reviewed and published; no mathematical or statistical doubts regarding the technique's accuracy or effectiveness have been raised by other professionals in the field.

Moreover, the statistical technique used in this case has been successfully used to investigate and prosecute federal cases. Exh. C at 11-12. As the Authors note in the 2020 Article, every court that has considered a motion to suppress challenging the methodology applied in the instant case has denied the motion. *See id*. In addressing a motion to suppress, the United States District Court for the Eastern District of Pennsylvania summarized the

methodology used by law enforcement to identify IP addresses that request child pornography as follows:

> A product of significant research and a deep knowledge of Freenet, the Algorithm is extraordinarily reliable, showing 98 to 100% accuracy in distinguishing between original requesters and relayers of Network files. This degree of accuracy compels the common-sense conclusion that Defendant was an original requester of the files he asks me to suppress. That conclusion is bolstered by the FBI's prudence in seeking a search warrant only after observing four attempted transmissions of child pornography files to the same Freenet user. Surely the likelihood is negligible that the Levine Algorithm failed repeatedly and that the same user happened to relay requests for child pornography files four times in five months (despite request characteristics indicating otherwise). The Agent's actions thus were manifestly reasonable.

United States v. Weyerman, No. 19-188, ECF No. 45, at 12 (E.D. Pa. filed Jan. 3, 2020) (internal citation omitted). Here, law enforcement sought a search warrant after observing nine attempted downloads of child pornography files. *See* DE #22-1 at 8-10.

In attacking the reliability of the statistical method, McEachern actually attacks the reliability of the formula described in the Black Ice Project, not the aforementioned statistical technique described in the Scientific Articles. *See* DE #22 at 14-18. The defendant accurately describes the randomization of the HTL values and the source code developed for rerouting each request. *Id*. at 14-16. The defendant focuses on examining the HTL values of requests for

blocks, and counting the number of HTL values of 16s, 17s, and 18s. DE #22 at 14-17. This is all information the Black Ice Project uses to try to track backwards toward the source. *See* DE #22-2. McEachern quotes the mathematical formula used by the Black Ice Project. DE #22 at 16. The Black Ice Project is not a peer-reviewed scientific article and it is not the statistical foundation used in this investigation. In fact, in the 2020 Article, the Authors prove that using the method described in the Black Ice Project does not reliably identify the original requester. Exh. C at 5. In support of his motion, McEachern provides as an exhibit the very article describing the statistical technique used to identify McEachern's IP address. *See* DE #22-3.

In short, the government agrees that the mathematical formula described by the Black Ice Project is arbitrary, inaccurate and unreliable. However, that method was not used during the investigation of the instant case. The concern raised by the motion is therefore unfounded.

To the extent that McEachern argues that the affidavit does not show sufficiently how the statistical technique was used to identify McEachern as the original requester, the argument fails. The affidavit describes the statistical technique and how it was applied to McEachern. The affidavit includes: a) a description of Freenet; b) a description of how Freenet operates when it attempts to download a file; c) that the manner in which it operates

when making a request can help distinguish between a user that is an original requester and one that is a relayer; d) that law enforcement has a modified version of Freenet software that automatically logs information about requests for pieces of files received by peers; e) that there is a mathematical formula that can be applied to identify the original requester; f) there is a mathematical formula that can be applied to data from the logs to determine who is the significantly more likely to be the original requester; g) the formula was applied to nine separate files of interest in September and October 2021; and h) precise observed values of average peers, requested pieces and total pieces need to assemble the file for each child pornography file of interest. DE #22 at 4-12.

McEachern's last argument related to heavy Freenet traffic effecting the reliability also fails because of its reliance on the mathematical formula described in the Black Ice Project, as described above. To the extent that the defendant argues that heavy traffic on the Freenet Network would affect the reliability of the statistical technique described in the Scientific Articles, the argument also fails. *See* DE #22 at 18. The 2020 Article included an experiment that measured the false positive rate of the technique that was used in this investigation. Exh. C at 8-9. The real-world implementation of the technique in the high volume traffic resulted in reducing the previously

calculated false positive rate to less than 1%. *Id*. In the presences of the high-volume requests for child pornography, the technique was extremely reliable.

B. Special Agent White Acted with Good Faith

Even where courts find that a warrant was not supported by probable cause, the Fourth Amendment contains no "provision expressly precluding the use of evidence obtained in violation of its commands." *United States v. Leon*, 468 U.S. 897, 906 (1984). Instead, suppression is a "judicially created remedy designed to safeguard Fourth Amendment rights through its deterrent effect." *Id*. However, suppression does not achieve deterrence where the officer acted with objective good faith. *See United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011) (citation omitted). Therefore, courts "should not suppress the fruits of a search conducted under the authority of a warrant, even a 'subsequently invalidated' warrant, unless 'a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Bynum*, 293 F.3d 192, 195 (4th Cir. 2002) (quoting *Leon*, 468 U.S. at 922 n.23). To that end, under the good faith exception to the exclusionary rule, suppression is "inappropriate" where an affidavit can produce "disagreement among thoughtful and competent judges as to the existence of probable cause." *Bosyk*, 944 F.3d at 333.

Leon identified four situations where an officer's reliance on the warrant

is not objectively reasonable:

> (1) where the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) where the issuing magistrate wholly abandoned his judicial role as a detached and neutral decisionmaker; (3) where the officer's affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where a warrant [is] so facially deficient ... that the executing officers cannot reasonably presume it to be valid.

United States v. Andrews, 577 F.3d 231, 236 (4th Cir. 2009), internal quotations and citation omitted, alteration in original.

McEachern assertions provide no basis to conclude that any of the circumstances are present here. White's affidavit is far from the type of "bare bones" affidavit that renders police relance objectively unreasonable. As detailed above, White explained his background, training, experience and familiarity with computer crimes; described Freenet and the modified law enforcement version of the software that logged data and that you could apply a "mathematical formula" to that data "to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request to another computer;" detailed the application of the "mathematical formula" to data logged from the requesting user; and explained the probable cause that

resulted in McEachern's residence being identified. *See* DE #22-1.

Even if there were facts that could have been added to the affidavit, the Fourth Circuit has reasoned that "agents need not include disclaimers specifically pointing out facts absent from the affidavit to obtain a warrant. A warrant application is 'judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added.'" *Bosyk*, 9233 F.3d at 332. The *Bosyk* court also explained that "a defendant can't suppress evidence on grounds that the affiant intentionally or recklessly omitted facts without first making 'a substantial preliminary showing' to that effect. And importantly, that showing requires 'a detailed offer of the missing information." *Bosyk*, 933 F.3d at 33 (citations omitted). McEachern does not present a detailed offer of proof, because he does not have one.

Failure to explain the methodology of identifying requesting IP addresses has not resulted in the suppression of evidence recovered based on the search warrant being challenged. Even when an affiant did not include any details about "Dr. Levine, his algorithm, or how officers use the algorithm to determine which Freenet users requested which files," *United States v. Dickerman*, 954 F.3d 1060, 1064 (8th Cir. 2020), the Eighth Circuit upheld the search warrant in a Freenet investigation because the officers' reliance on the warrant was "objectively reasonable. [The affiant] did not make the conclusion

that Dickerman was a requester in isolation: he supported it with other detailed facts about the officers' understanding of Freenet's functionality, their qualifications in computer forensics and experience investigating peer-to-peer networks, and Dickerman's Freenet use," *id.* at 1067 (affirming the district court's denial of the defendant's motion to suppress based on the good-faith exception and not reaching the underlying question of probable cause). The Sixth Circuit has similarly affirmed the district court's denial of a motion to suppression when confronted with this issue, explaining that "the omission of information regarding the reliability of the [law enforcement] software does not call into question the reliability of this software and does not provide grounds for an evidentiary. Furthermore, it is arguable that such information would have only strengthened the affidavit by showing that the software was reliable." *United States v. Dunning*, 857 F.3d 342, 347 (6th Cir. 2017) (citation omitted).

III. CONCLUSION

The warrant established probable cause. Assuming *arguendo* that it did not, the good faith exception applies. McEachern's motion is meritless and should be denied.

This the 8th day of April, 2022.

SANDRA J. HAIRSTON
United States Attorney

/S/ K. P. KENNEDY GATES
Assistant United States Attorney
NCSB No.: 41259
United States Attorney's Office
101 S. Edgeworth St., 4th Floor
Greensboro, NC 27401
336/333-5351

CERTIFICATE OF SERVICE

I hereby certify that on April 8, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the following:

Helen L. Parsonage, Esq.

SANDRA J. HAIRSTON
United States Attorney

/S/ K. P. KENNEDY GATES
Assistant United States Attorney
NCSB No.: 41259
United States Attorney's Office
101 S. Edgeworth St., 4th Floor
Greensboro, NC 27401
336/333-5351